United States Senate
Committee on Homeland Security and Governmental Affairs
Chairman Joseph I. Lieberman, ID-Conn.

Opening Statement for Chairman Joseph Lieberman
Hearing, "Securing Critical Infrastructure in the Age of Stuxnet"
Homeland Security and Governmental Affairs Committee
November 17, 2010

Good morning, the hearing will come to order. This is a hearing to both remind us and educate those who are watching about the reality of the cyber threat to the United States and how important it was that we worked hard to develop cyber security reform legislation in this committee. It's unfortunate that the clock will run out on us before we have a chance to complete negotiations with other committees and with the administration, who I regret to say did not engage as early in the process of developing this legislation as was necessary.

But this Stuxnet story really takes the reality of the threat to a new level and should awaken any skeptics. There are some who think we're overstating the threat and therefore overreacting in the public resources that we're devoting to the protection of our cyber systems here in America. Of course I totally disagree with that argument.

We have an extraordinary group of witnesses here today, who will not only tell us what Stuxnet is, but will help talk more generally about the cyber threat to our country.

I want to say, in terms of our legislation, that it's certainly my intention to come back to this legislation early in the next congress and try to get it out as soon as possible. Again, I want to say that this will require more immediate and intense concentration by the Administration and by some of the other committees that claim jurisdiction here. We of course are the ultimate source of jurisdiction for cyber security that is non-defense, which is the Armed Services Committee. This will be a real priority for the Committee when the new Congress begins next year.

<u>The Following Was Entered Into the Hearing Record:</u>

Last summer, a dangerous piece of malicious software, or "malware," was discovered that dwarfed almost anything that has come before it, both in sophistication and destructive potential.
Named Stuxnet, it specifically targets computers that run the industrial systems used to control electric, water treatment, nuclear and chemical plants, as well as pipelines, communications, transportations, manufacturing systems and other critical infrastructure.

Stuxnet is a dual menace. First, it has the power to burrow deep into a network and steal secrets. Second, and most frightening, it also has the ability to commandeer industrial operations and make machinery do things – like open or close a valve – undetected by a plant's operators because Stuxnet tells the operators their instructions are being followed.

The potential for catastrophic consequences should these critical systems fall under the control of our enemies is obvious. But prior to Stuxnet, many considered the probability of this kind of attack on a large-scale system to be remote.

This Committee has already held several hearings on cyber security, during which we heard about cyber crime and cyber espionage.

In those hearings we discussed denial of service attacks that shut down commercial websites and phishing schemes that tricked people into giving away crucial information that could then be used to empty corporate bank accounts or steal industrial or national secrets.

But these attacks are primitive compared to Stuxnet – like muskets versus a machine gun.
Our witnesses will be offering a more detailed technical analysis of Stuxnet, but I wanted to touch on just a few things to give an idea of its size and sophistication.

Experts estimate that 10,000 man-hours of programming time went into writing Stuxnet as a seamless piece of code, and its authors would have had to be experts both in Microsoft's operating systems and in the much more esoteric systems and computer languages that control industrial systems.

Put differently, Stuxnet was created by a team that could speak both English and Urdu with complete fluency.

Stuxnet has some 4,000 functions, not all of which have been documented yet. By comparison, the software that runs the average e-mail server has about 2,000 functions.

Stuxnet invades its target computers using four different Microsoft Windows security vulnerabilities that had been unknown until Stuxnet was set loose.

These security flaws, known as "zero-day vulnerabilities," are difficult to discover and are valuable commodities on the black market. Using four of them in one piece of malware is unprecedented.
And Stuxnet will even update itself automatically if it runs into a newer version on another computer.

So we know that Stuxnet is highly sophisticated and complex. What we don't know, despite much speculation, is who created Stuxnet or why.

So far, Stuxnet has done no known damage. But that doesn't mean it won't. It may still be looking for its ultimate target or, it may have already found it and is simply lying in wait for the precise set of events that will trigger its more destructive capabilities.

Experts continue to work on this problem but that is not our focus today. The very fact that Stuxnet exists shows that we can no longer pretend that a cyber attack on our critical infrastructure is hypothetical or hyperbolic.

It is possible that other malicious hackers could use Stuxnet as a blueprint to create even more destructive malware.

Our concern today is what Stuxnet tells us about the state of security of our critical infrastructure and what role the federal government should play in this new age of cyber warfare, where the targets are not just naval fleets or military bases, but strategic computer network systems that are almost entirely in the hands of the private sector.

This is no small difference. The private sector evaluates risk differently than the government. A single industrial network, say an electric plant, might look at the cost of security and say: "What is the minimum I must do to protect the system and not hurt my bottom line."

Downtime is expensive, which is why the average industrial system is off line for just four hours a year for maintenance. And if a system is only rarely taken down, it is all the more difficult to install patches from newly discovered vulnerabilities.

The federal government has to take the broader view and look at how we defend the economy and the computer infrastructure that supports it as a whole and create standards to accomplish that.

Legislation Sen. Collins and I have proposed would give the federal government modern tools to secure and defend the nation's most critical cyber networks and establish public/private partnerships that will help set those kinds of national cyber security priorities.

Most relevant to this hearing are the provisions that would establish a National Center for Cybersecurity and Communications – or N Triple C – within the Department of Homeland Security and empower that Center to help secure critical infrastructure networks, like utilities and communications systems.

The reality is that the current, porous state of our nation's infrastructure means that it wouldn't take malware as robust and sophisticated as Stuxnet to cripple many of our critical systems.

Consequently, our legislation will raise the security bar for all systems, making attacks more difficult, and will put in place processes that will help remediation after a successful attack.

I'm sorry to say it seems unlikely we can pass this bill in this lame duck session, although we should. I've been disappointed that the Administration and some other Committees that have an interest in this issue have been slow to engage.

But with that said, we have made a lot of progress on it and I hope in the next session of Congress we can pick up where we left off and quickly enact this legislation that is crucial to public safety and our economic and national security.

Stuxnet was the warning of a gathering storm. We ignore it at great peril.

Sen. Collins.

-30-